CLAIMS:

Sub a1

1. A method of updating a communications key maintained in a unit for communicating with a communications system, said method comprising:

generating a new communications key using a secret value stored in said unit;

generating an update key using said secret value stored in said unit;

performing an authentication using said update key; and

updating said communications key with said new communications key after said authentication.

2. The method of claim 1 comprising:

receiving an update sequence;

generating said new communications key using a secret value stored in said unit and said sequence;

generating a signature value using said update key; and

comparing said signature value with a signature value received from said communications system which was generated using said update key to perform said authentication.

3. The method of claim 2 further comprises:

generating a challenge sequence;

sending said challenge sequence to said communications system;

generating said signature value using said challenge sequence and said update key;

receiving a signature string generated by said communications system using said challenge sequence and said update key; and

comparing said signature value with said signature value generated by said communications system.

4. The method of claim 3 comprises:

generating a second signature value using said update sequence and said update key; and

sending said second signature value to said communications system for comparison with a second signature value generated by said communications system using said sequence and said update key generated at said communications system.

5. The method of claim 3 wherein said generating said signature value includes:

developing a signature string comprising at least portions of said update sequence, said challenge sequence and said update key; and

generating said signature value from at least said signature string.

6. The method of claim 4 wherein said generating said signature value includes:

developing a second signature string comprising at least portions of said update sequence, said challenge sequence and said update key; and

generating said second signature value from at least said second signature string.

7. A method of updating a communications key maintained in a unit and in a communications system, said method comprising:

sending to said unit an update sequence for said unit to generate a new communications key using a secret value in said unit;

sending to said unit a signature value for said unit to compare said signature value generated at said communications system using an update key derived from a secret value stored in said communications system associated with said unit; and

receiving an update confirmation after which said communications key is updated with said authentication.

8. The method of claim 7 comprising:

generating said signature value.

9. The method of claim 8 wherein said generating a signature value including:

receiving a challenge sequence from said unit; and

generating said signature value using said challenge sequence and said update key.

10. The method of claim 9 including:

generating a second signature value using said update sequence and said update key; and

receiving a second signature value generated at said unit using said update sequence and said update key at said unit;

comparing with said second signature value with said second signature value generated by said unit.

11. The method of claim 10 wherein said generating a signature value including:

developing a signature string comprising at least portions of said update sequence, said challenge sequence and said update key; and

generating said signature value from at least said signature string.

12. The method of claim 10 wherein said generating a second signature value including:

developing a second signature string comprising at least portions of said update sequence, said challenge sequence and said update key; and

generating said second signature value from at least said second signature string.

13. A method of updating a communications key maintained in a unit and in a communications system, said method comprising:

generating an update sequence; and

generating a new communications key using a secret value stored in said communications system and associated with said unit and said update sequence;

generating an update key using said secret value and said update sequence;

updating said communications key with said new communications key after an authentication is performed with said unit using said update key.

14. The method of claim 13 further comprising:

providing said update key to generate a signature value using said update key in said communications system to compare at said unit said signature value with a signature value generated at said unit using an update key generated at said unit using said update sequence and a secret value stored in said unit; and

updating said communications key with said new communications key after receiving the results of said comparison of said signature values.

15. A method of updating a communications key maintained in a unit and in a home communications system, said method comprising:

receiving an update sequence from said home communications system for said unit to generate a new communications key using a secret value in said unit;

receiving an update key from said from said home communications system and generated at said home communications system using a secret value associated with said unit at said home communications system;

performing an authentication with said unit using said update sequence; and

sending to said home communications system the results of said authentication.